Instituto Tecnológico de Cancún

Materia:

Fundamentos de Telecomunicaciones

Tarea:

Investigación:

-Tipos de proxy

-MITM

Alumno: **Aguilar Moreno Jorge Axel**

Docente: **Ismael Jiménez Sánchez**

Horario: **17:00 – 18:00**

Ing. **Sistemas Computacionales**

5.-Semestre

Qué es un proxy

En primer lugar, vamos a empezar hablando de qué es un proxy. Un servidor proxy es un servidor (puede ser tanto un programa como un dispositivo físico) que actúa como un intermediario. Se sitúa entre la solicitud que realiza un cliente y otro servidor que da la respuesta. Si queremos acceder desde un móvil a un servidor de Internet donde está alojada una página web, un proxy puede actuar de intermediario.

Esto permite ganar más control de acceso, registrar el tráfico o incluso restringir determinados tipos de tráfico. De esta forma podremos mejorar en seguridad y también en rendimiento, así como tener anonimato al acceder a determinados servicios.

Una de las funciones más comunes para lo que los usuarios utilizan los proxys es para saltarse la restricción geográfica. Es decir, un proxy puede actuar como intermediarios y hacer que nuestra conexión aparezca en otro lugar. De esta forma podemos acceder a contenido disponible únicamente para un determinado país o poder ver contenido que no esté disponible en el nuestro.

Qué tipos de proxys existen

Ahora bien, hay que tener en cuenta que existen diferentes tipos de proxys. Vamos a ver cuáles son los más comunes.

Proxy web

Sin duda uno de los servidores proxy más populares son los web. Estamos ante una opción en la que los usuarios pueden acceder a través de una página web. Esa web es la que actúa como proxy. Está basado en HTTP y HTTPS y actúa como intermediario para acceder a otros servicios en Internet.

A través de esa página web podremos navegar por otros sitios. Toda esa navegación pasa a través del proxy web que estamos utilizando.

Proxy caché

Otra opción es la de un servidor proxy caché. En este caso este servidor actúa como intermediario entre la red e Internet para cachear contenido. Puede ser contenido de tipo estático como HTML, CSS, imágenes… Se utiliza para acelerar el contenido de un sitio al navegar.

Si una persona entra en una página por segunda vez, esa información que está cargando ya puede estar cacheada. De esta forma no necesita descargarla de nuevo y va más rápido.

Proxy reverso

También están los proxys reversos. Puede utilizarse para brindar acceso a Internet a un usuario en concreto dentro de la red, ofrecer algún tipo de caché o incluso actuar como firewall y ayudar a mejorar la seguridad.

Proxy transparente

En este caso lo que hace el proxy es obtener la petición que hemos dado y darle una redirección sin necesidad de modificar nada previamente. Básicamente actúa como un intermediario sin modificar nada, de ahí el nombre que obtiene.

Proxy NAT

Una opción más en cuanto a proxys es los proxys NAT. Principalmente se utilizan para enmascarar la identidad de los usuarios. Esconde la verdadera dirección IP para acceder a la red. Cuenta con variadas configuraciones.

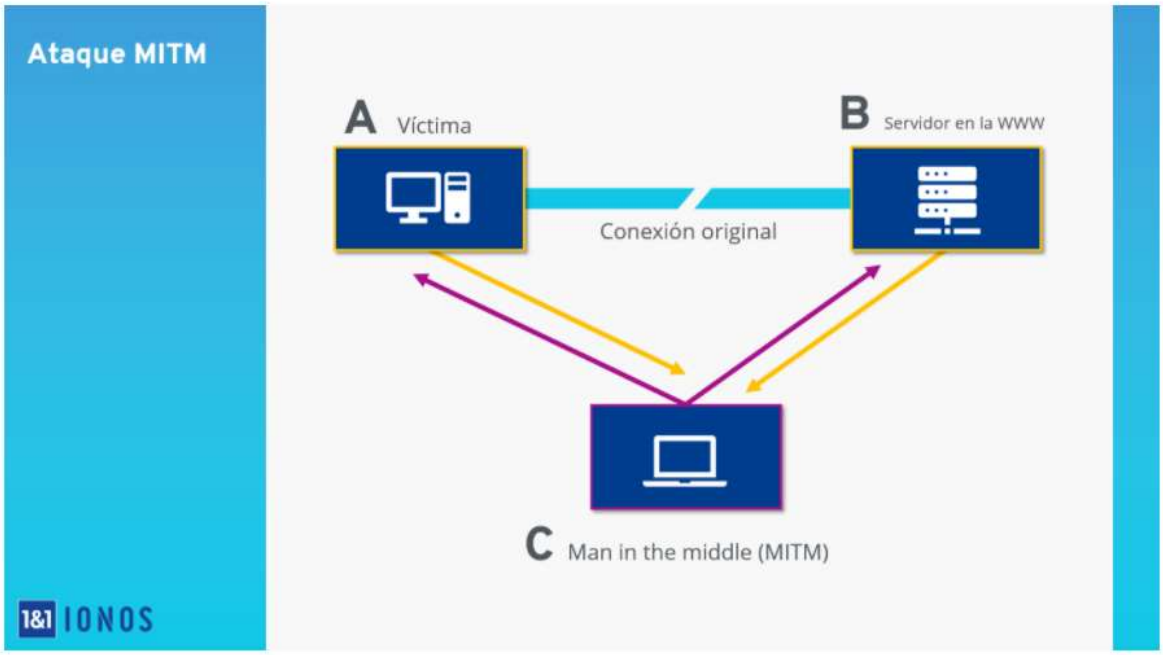
En definitiva, estos son los principales tipos de proxys que podemos encontrarnos. Como vemos hay una variedad de opciones y cada uno de ellos puede tener un uso diferente de cara a los usuarios. Todos ellos actúan como intermediarios entre el usuario (dispositivo móvil, ordenador…) y un servidor. Pueden ayudar para mejorar la seguridad y privacidad, así como para obtener diferentes funciones a la hora de navegar por la red.

MITM (MAM IN THE MIDDLE)

¿Qué es un ataque Man in the Middle?

Por su nombre en inglés, un intermediario, normalmente el cibercriminal o un software malicioso, se incrusta entre la víctima y la fuente de datos (cuentas bancarias, email…etc.). El objetivo es interceptar, leer o manipular de forma efectiva la comunicación entre la víctima y sus datos sin que nadie se dé cuenta de que hay una tercera persona incluida en la operación.

El gráfico que aparece a continuación, ilustra el **esquema básico de un ataque man-in-the-middle.**



Esquema gráfico de un ataque MitM: el sistema C interviene sin ser percibido en la comunicación entre el sistema A y el sistema B.

El sistema A intenta crear una conexión codificada con el sistema B pero, en lugar de ello, un tercer partido malintencionado desvía el flujo de datos para establecer la conexión codificada del sistema A con el sistema C y que a partir de ahí se transmita al sistema B. Esto tiene como consecuencia que aquel que tenga el control sobre el sistema C (el atacante generalmente) puede examinar, grabar o manipular el tráfico de datos, a menudo incluso sin que los participantes en la comunicación sean conscientes de ello. Una vez hecha la transmisión a la World Wide Web, el sistema

C se presentará como servidor web ante el sistema A y como navegador web ante el sistema B.

Modalidades de ataque man-in-the-middle

Para infiltrase en el tráfico de datos entre dos o más sistemas, los hackers recurren a diversas técnicas que se centran en las debilidades de la comunicación por Internet.

- **Ataques basados en servidores DHCP**

  En el caso de los ataques basados en un servidor DHCP, es un hacker el que coloca su propio ordenador (o uno que esté bajo su control) en una red de área local (LAN) a modo de **servidor DHCP**.

- **ARP Cache poisoning**

  Por ARP (Address Resolution Protocol) se entiende aquel protocolo de red que sirve para resolver direcciones IP de redes LAN en direcciones de hardware (direcciones MAC).

- **Ataques basados en servidores DNS**

  Mientras que el ARP cache poisoning fija su atención en las debilidades de la resolución de direcciones en Ethernet, la prioridad del envenenamiento del caché basado en servidores DNS es el **sistema de nombres de dominio** de Internet, que es el responsable de la resolución de URL en direcciones IP públicas.

- **Simulación de un punto de acceso inalámbrico**

  Un modelo de ataque dirigido sobre todo a los usuarios de dispositivos móviles se basa en la **simulación de un punto de acceso inalámbrico** en una red inalámbrica pública, como las de las cafeterías o las de los aeropuertos.

- **Ataque MAINT IN THE BROWSER**

  El **ataque man-in-the-browser** es una variante del ataque MitM. En él, el atacante instala malware en el navegador de los usuarios de Internet con el objetivo de interceptar sus datos.

- **Human Assisted Attack**

  Se puede hablar de human assisted attack cuando una de las modalidades de ataque anteriores no se realiza de manera automática, sino de la mano de uno o varios atacantes en tiempo real.

Cómo prevenir los ataques man-in-the-middle

Por norma general es casi imposible que los afectados puedan reconocer la presencia de un ataque de intermediario, por lo que la prevención se convierte en la mejor forma de protección. A continuación, presentamos una recopilación de los consejos más importantes para que los usuarios de Internet y operadores de páginas web puedan minimizar el riesgo de convertirse en blanco de un ataque MitM.

Consejos para usuarios de Internet

- ✓ Asegúrate de acceder siempre a los sitios web con una conexión segura SSL/TLS. Mientras que las direcciones de Internet que empiezan con https son seguras, las que lo hacen con http suponen un riesgo para la seguridad.
- ✓ Antes de introducir las credenciales, comprueba si el certificado SSL de un sitio web está actualizado y ha sido emitido por una autoridad de certificación de confianza.
- ✓ El navegador ha de utilizarse siempre en su última versión y el sistema debe estar al día con las actualizaciones.
- ✓ Evita usar redes VPN de acceso libre o servidores proxy.
- ✓ Mantén las contraseñas actualizadas, utiliza para cada aplicación una contraseña diferente y evita utilizar contraseñas antiguas.
- ✓ Evita conectarte a redes wifi abiertas, por ejemplo, en hoteles, estaciones de tren o tiendas.
- ✓ Si no tienes más remedio que acceder a una red pública, evita descargar información, transmitir datos de inicio de sesión (por ejemplo, para la bandeja de entrada del correo electrónico o redes sociales) y realizar algún pago.
- ✓ Si el operador de un sitio web ofrece métodos adicionales para iniciar sesión de forma segura, utilízalos. Entre ellos pueden citarse la autenticación multifactorial (MFA) a través de un token, por SMS o vía app en el smartphone.

- ✓ No cliques en los enlaces de correos de remitentes desconocidos, pues pueden dirigirte a un sitio web con malware.

Consejos para operadores de sitios web

- Protege siempre los datos de tus clientes con un certificado SSL actualizado de una autoridad fiable en páginas web con acceso para clientes.
- Ofrece a tus usuarios métodos adicionales para que puedan iniciar sesión de forma segura. Por ejemplo, con una autenticación multifactor a través del correo.
- Haz saber a los clientes que, en principio, nunca vas a pedir los datos de acceso a través del email y evita los enlaces en los correos que les envíes.

Referencias:

- https://www.redeszone.net/noticias/redes/palo-alto-servicio-perdida-datos-nube/
- https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/
- https://www.ionos.mx/digitalguide/servidores/seguridad/ataques-man-in-the-middle-un-vistazo-general/